Microsoft Windows Server 2003 Certificate Service

Microsoft Deutschland GmbH

ISIS-MTT-Assessment Report

Version 1.0
Date 10. März 2004

Holger Mack, Dr. Markus Michels

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Secorvo herewith confirms, that for the product

Microsoft Windows Server 2003 Certificate Service

manufactured by

Microsoft Corporation

One Microsoft Way, Redmond, WA 98052-6399, USA

an ISIS-MTT-compliance assessment has been completed between March 8 to March 9, 2004.

The product is ISIS-MTT-compliant with respect to the Component Conformance Statement ref. no Secorvo-00003 provided

We recommend to award the

ISIS-MTT-conformance label ("ISIS-MTT Siegel")

for the

product class "CA Server"

Reference-Number: *Secorvo-00003*

ISIS-MTT Specification Version: 1.1 (Draft)

ISIS-MTT Test Specification Version: 1.0.2

ISIS-MTT Compliance Criteria Version 1.1

ISIS-MTT Testbed Version: Release 1.1 Build 5 SP1 (with modifications)

Karlsruhe, March 9, 2004.

Holger Mack

Content

1 Summarized Assessment Results 5
2 Testgroup GEN-CERT 6
2.1 Test Case TCGPKC-1 6
2.1.1 Issuer Certificate 6
2.1.2 Sub-CA Certificate 6
2.1.3 End Entity Certificate 7
2.2 Test Case TCGDNAMES-1 8
2.2.1 Issuer Certificate 8
2.2.2 Sub-CA Certificate 9
2.2.3 End Entity Certificate 10
2.2.4 CRL 10
2.2.5 Delta-CRL 11
2.3 Test Case TCGEXTENSIONS-1 11
2.3.1 Issuer Certificate 11
2.3.2 Sub-CA Certificate 12
2.3.3 End Entity Certificate 13
2.3.4 CRL 14
2.3.5 Delta-CRL 15
2.4 Test Case TCGCRL-1 15
2.4.1 CRL 15
2.4.2 Delta-CRL 16
3 Technical Data 18
4 Test Procedure 19
4.1 Installation 19
4.2 Configuration 19
4.3 Preparation of the tests 19
4.4 Performing the tests 19
4.4.1 Template ISIS-MTT Assessment User 19
4.4.2 Template ISIS-MTT Assessment Sub CA 20
4.5 Modifications in the Capolicy.inf File 20
5 Component Conformance Statement 21
6 Annex I: Test Log 24
6.1 Issuer Certificate 24

6.2 Sub CA Certificate 27
6.3 End Entity Certificate 30
6.4 CRL 34
6.5 Delta-CRL 37

Acronyms

AC	Attribute Certificate
ASN.1	Abstract Syntax Notation no. 1
CA	Certification Authority
CMC	Certificate Management protocol using CMS
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
EE	End Entity
FC	Functionality Class
HTTP	HyperText Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standard
SigG	Signaturgesetz [(German) Signature Law]
S/MIME	Secure / Multipurpose Internet Mail Extensions
SP	Service Pack
TSP	Time Stamp Protocol

1 Summarized Assessment Results

The product falls into product class “CA Server”. Functionality classes 1 and 4 are declared to be conformant to ISIS-MTT and were tested during the compliance assessment.

All tests were passed, some with warning. The overall result of the assessment is “**passed**”.

These are the summarized results:

FC	Description	Result
1	Generation of public key certificates	passed with warning
4	Generation of CRLs	passed with warning

Note: The tests were based on the ‘ISIS-MTT Specification Part 1 Certificate and CRL Profile Version 1.1, draft’ (document *ISIS-MTT_Part1_CertAndCrlProfile_v1.1DRAFT_07.pdf*) as published for commenting. This assessment assumes that this draft is agreed by the ISIS-MTT board without changes relevant for this assessment. Other parts of the ISIS-MTT standard are not relevant for this assessment.

The tests were performed using the ISIS-MTT testbed implementing the version 1.02 of the ISIS-MTT specification. Therefore some test steps are marked as ‘failed’, however these issues are resolved by the changes made in version 1.1 (draft). Explanations are given with the individual test steps.

None of the modification in the draft for version 1.1 has a negative effect on any test steps marked as passed by the test-bed.

2 Testgroup GEN-CERT

In the following the tests results are summarized. For more details, see Annex I: Test Log.

2.1 Test Case TCGPKC-1

2.1.1 Issuer Certificate

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed
Test step 6 (issuer)	failed (see Note)
Test step 7 (validity)	passed
Test step 8 (subject)	failed (see Note)
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueID)	passed
Test step 11 (subjectUniqueID)	passed
Test step 12 (extensions)	passed with warning

Test case passed with warnings

Note: The failure steps 6 and 8 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the issuer certificate. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and after. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus these test cases are passed.

2.1.2 Sub-CA Certificate

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed

Test step 6 (issuer)	failed(see Note)
Test step 7 (validity)	passed
Test step 8 (subject)	failed(see Note)
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueID)	passed
Test step 11 (subjectUniqueID)	passed
Test step 12 (extensions)	failed (see Note)

Test case passed with warnings

Notes:

The failure steps 6 and 8 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the Sub-CA certificate. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and after. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus these test cases are passed.

The failure in step 12 is due to the use of the Access Method “caIssuer” in the AuthorityInfoAccess extension. While this method is forbidden in the ISIS-MTT specification 1.0.2, it is allowed in the version 1.1 (Draft). Therefore this test case is passed (with warning).

2.1.3 End Entity Certificate

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed
Test step 6 (issuer)	failed (see Note)
Test step 7 (validity)	passed
Test step 8 (subject)	failed (see Note)
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueID)	passed
Test step 11 (subjectUniqueID)	passed
Test step 12 (extensions)	failed (see Note)

Test case passed with warning

Notes:

The failure steps 6 and 8 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the Sub-CA certificate. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and after. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus these test cases are passed.

The failure in step 12 is due to the use of the Access Method “caIssuer” in the AuthorityInfoAccess extension. While this method is forbidden in the ISIS-MTT specification 1.0.2, it is allowed in the version 1.1 (Draft). Therefore this test case is passed (with warning).

2.2 Test Case TCGDNAMES-1

2.2.1 Issuer Certificate

2.2.1.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the issuer name in the issuer certificate is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.1.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the subject name in the issuer certificate is due to the requirement that all name attributes shall be encoded in UTF8 format

in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.2 Sub-CA Certificate

2.2.2.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the issuer name in the Sub-CA certificate is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.2.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the subject name in the Sub-CA certificate is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.3 End Entity Certificate

2.2.3.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the subject name in the end entity certificate is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.3.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the subject name in the end entity certificate is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.4 CRL

2.2.4.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the subject name in the CRL is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.2.5 Delta-CRL

2.2.5.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

Test case passed

Note: The failure in test step 2 of the test TCGDNAMES-1 for the subject name in the Delta-CRL is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and afterwards. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.3 Test Case TCGEXTENSIONS-1

2.3.1 Issuer Certificate

Test step 1 (all extensions)	passed with warning
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 3 (SubjectKeyIdentifier)	passed
Test step 4 (KeyUsage)	passed
Test step 5 (PrivateKeyUsagePeriod)	passed

Test step 6 (CertificatePolicies)	passed
Test step 7 (SubjectAltNames)	passed
Test step 8 (IssuerAltNames)	passed
Test step 9 (SubjectDirectoryAttributes)	passed
Test step 10 (BasicConstraints)	passed
Test step 11 (NameConstraints)	passed
Test step 12 (PolicyConstraints)	passed
Test step 13 (ExtendedKeyUsage)	passed
Test step 14 (CRLDistributionPoints)	passed
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

Test case passed with warning

2.3.2 Sub-CA Certificate

Test step 1 (all extensions)	passed with warning
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 3 (SubjectKeyIdentifier)	passed
Test step 4 (KeyUsage)	passed
Test step 5 (PrivateKeyUsagePeriod)	passed
Test step 6 (CertificatePolicies)	passed
Test step 7 (SubjectAltNames)	passed
Test step 8 (IssuerAltNames)	passed
Test step 9 (SubjectDirectoryAttributes)	passed
Test step 10 (BasicConstraints)	passed
Test step 11 (NameConstraints)	passed
Test step 12 (PolicyConstraints)	passed

Test step 13 (ExtendedKeyUsage)	passed
Test step 14 (CRLDistributionPoints)	passed
Test step 15 (AuthorityInfoAccess)	failed (see Note)
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

Test case passed with warning

Note: The failure in step 15 is due to the use of the Access Method “caIssuer” in the AuthorityInfoAccess extension. While this method is forbidden in the ISIS-MTT specification 1.0.2, it is allowed in the version 1.1 (Draft). Therefore this test case is passed (with warning).

2.3.3 End Entity Certificate

Test step 1 (all extensions)	passed with warning
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 3 (SubjectKeyIdentifier)	passed
Test step 4 (KeyUsage)	passed
Test step 5 (PrivateKeyUsagePeriod)	passed
Test step 6 (CertificatePolicies)	passed
Test step 7 (SubjectAltNames)	passed
Test step 8 (IssuerAltNames)	passed
Test step 9 (SubjectDirectoryAttributes)	passed
Test step 10 (BasicConstraints)	passed
Test step 11 (NameConstraints)	passed
Test step 12 (PolicyConstraints)	passed
Test step 13 (ExtendedKeyUsage)	passed with warning
Test step 14 (CRLDistributionPoints)	passed
Test step 15 (AuthorityInfoAccess)	failed (see Note)
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed

Test step 18 (OCSPNocheck)	passed

Test case passed with warning

Note: The failure in step 15 is due to the use of the Access Method “caIssuer” in the AuthorityInfoAccess extension. While this method is forbidden in the ISIS-MTT specification 1.0.2, it is allowed in the version 1.1 (Draft). Therefore this test case is passed (with warning).

2.3.4 CRL

2.3.4.1 CrlEntryExtensions

Test step 1 (all extensions)	passed
Test step 22 (ReasonCode)	passed
Test step 23 (HoldInstructionCode)	passed
Test step 24 (InvalidityDate)	passed
Test step 25 (CertificateIssuer)	passed

Test case passed

2.3.4.2 CRLExtension

Test step 1 (all extensions)	passed with warning
Test step 2 (AuthorityKeyIdentifier)	passed with warning
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 8 (IssuerAltNames)	passed
Test step 19 (CRLNumber)	passed
Test step 20 (DeltaCRLIndicator)	passed
Test step 21 (IssuingDistributionPoint)	passed

Test case passed with warning

2.3.5 Delta-CRL

2.3.5.1 CrlEntryExtensions

Test step 1 (all extensions)	passed
Test step 22 (ReasonCode)	passed
Test step 23 (HoldInstructionCode)	passed
Test step 24 (InvalidityDate)	passed
Test step 25 (CertificateIssuer)	passed

Test case passed

2.3.5.2 CRLExtension

Test step 1 (all extensions)	passed with warning
Test step 2 (AuthorityKeyIdentifier)	passed with warning
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 8 (IssuerAltNames)	passed
Test step 19 (CRLNumber)	passed
Test step 20 (DeltaCRLIndicator)	passed
Test step 21 (IssuingDistributionPoint)	passed

Test case passed with warning

2.4 Test Case TCGCRL-1

2.4.1 CRL

Test step 1.1 (parse ASN.1 CertificateList)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed

Test step 3 (signature)	passed
Test step 4 (issuer)	failed (see Note)
Test step 5 (thisUpdate)	passed
Test step 6 (nextUpdate)	passed
Test step 7 (revokedCertificates)	passed
Test step 7/a (userCertificate)	passed
Test step 7/b (revocationDate)	passed
Test step 7/c (crlEntryExtensions)	passed
Test step 8 (crlExtensions)	passed with warning

Test case passed with warning

The failure in step 4 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the CRL. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 and after. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postponed; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

2.4.2 Delta-CRL

Test step 1.1 (parse ASN.1 CertificateList)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 3 (signature)	passed
Test step 4 (issuer)	failed (see Note)
Test step 5 (thisUpdate)	passed
Test step 6 (nextUpdate)	passed
Test step 7 (revokedCertificates)	passed
Test step 7/a (userCertificate)	passed
Test step 7/b (revocationDate)	passed
Test step 7/c (crlEntryExtensions)	passed
Test step 8 (crlExtensions)	passed with warning

Test case passed with warning

The failure in step 4 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the Delta-CRL. This result is due to the requirement that all name attributes shall be encoded in

UTF8 format in 2004 and after. The product uses PrintableString instead. In the ISIS-MTT specification 1.1 (Draft) this requirement is postoned; UTF8 and Printable String are the allowed formats. Thus this test case is passed.

3 Technical Data

The following products have been used:

- Windows Server 2003 Enterprise Edition (German) with Microsoft Patch KB824146 and KB825119.
- Certificate Service (Part of the used Windows Server 2003)
- Active Directory with DNS server(Part of the used Windows Server 2003)
- ISIS-MTT Testbed Prototype Release 1.1 Build 5 SP1 (modified)

4 Test Procedure

4.1 Installation

On one machine a Windows Server 2003 Enterprise Edition (German) and the Microsoft Patches KB824146 and KB825119 were installed. The Active Directory, DNS server, application server and certificate service.

On another server the ISIS-MTT Testbed 1.1 SP 5 was installed with the following modification:
In order to deal with the long OID in the Microsoft Extension "Certificate Template Information", the value of the variable MAX_OID in dumpasn1 tool had to be changed from 32 to 64.

4.2 Configuration

All services were installed with standard configuration unless stated otherwise. The server was configured as

- Domain controller (Active Directory) for new domain (forest)
  - Domain name: isismtt-compl-test.secorvo.testlab.de
  - NETBIOS Domain-name: WIN2003CATEST
  - DNS Server
  - Application Server
- Certificate Service Configuration
  - Enterprise Root CA
  - Adapted capolicy.inf file (see section 4.5)

4.3 Preparation of the tests

A user was registered in the Active Directory and was granted the right to obtain a user certificate.

4.4 Performing the tests

The user and sub-CA certificates were requested via the standard certificate service web-pages. For both certificate types a certificate template was created that reflect the ISIS-MTT requirements.

4.4.1 Template ISIS-MTT Assessment User

- Based on standard “Benutzer”-Template
- Relevant modifications:
  - Key Usage set as critical

- UPN not part of SubjectAltName

4.4.2 Template ISIS-MTT Assessment Sub CA

- Based on template “Untergeordnete Zertifizierungsstelle”
- Relevant modifications
  - Key Usage “Digital Signature” omitted
  - Key Usage set as critical

4.5 Modifications in the Capolicy.inf File

The following Capolicy.inf File was used:

```
[Version]
Signature="$Windows NT$"

[Extensions]
;
;The Extensions section marks the KeyUsage as critical
;
2.5.29.15=AwIBBg==
Critical=2.5.29.15
```

5 Component Conformance Statement

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: MICROSOFT WINDOWS SERVER 2003 CERTIFICATE SERVICE 2.0, MICROSOFT CORPORATION				
REFERENCE NUMBER: SECORVO-00003				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
	Generation and processing of certificates and CRLS			
1	Generation of public key certificates	☒	☐	
2	Generation of attribute certificates	☐	☒	
3	Generation of cross certificates	☐	☒	
4	Generation of CRLs	☒	☐	
5	Processing of public key certificates	☐	☒	
6	Processing of attribute certificates	☐	☒	
7	Processing of cross certificates	☐	☒	
8	Processing of CRLs	☐	☒	
	CMC			
9	“Simple CMC” in EEs	☐	☒	
10	“Simple CMC” in CAs	☐	☒	
	Generation and processing of S/MIME messages			
11	Generation of an S/MIME Message for Enveloped Data	☐	☒	
12	Generation of an S/MIME Message for Signed Data	☐	☒	
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	☐	☒	
14	Generation of a Multipart/Signed S/MIME Message	☐	☒	
15	Processing of a S/MIME message for enveloped-data	☐	☒	
16	Processing of S/MIME messages with signed data	☐	☒	
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	☐	☒	
18	Processing of a Multipart/Signed S/MIME message	☐	☒	
19	File signature and encryption	☐	☒	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: MICROSOFT WINDOWS SERVER 2003 CERTIFICATE SERVICE 2.0, MICROSOFT CORPORATION				
REFERENCE NUMBER: SECORVO-00003				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
20	**LDAP**			
21	LDAP client	☐	☒	
22	LDAP server	☐	☒	
	OCSP-Clients and Servers			
23	Transport of an OCSP Request	☐	☒	
24	Retrieval of OCSP responses	☐	☒	
25	Retrieval of an OCSP request	☐	☒	
26	Transport of an OCSP response	☐	☒	
	TSP			
27	TSP client	☐	☒	
28	TSP server	☐	☒	
	Certificate path validation			
29	Processing of a valid, 3-step certificate path	☐	☒	
30	Processing of an invalid certificate path	☐	☒	
	ISIS-MTT SigG-Profile			
31	Generation of SigG-conforming PKCs	☐	☒	
32	Generation of SigG-conforming ACs	☐	☒	
33	Processing of SigG-conforming PKC	☐	☒	
34	Processing of SigG-conforming ACs	☐	☒	
35	Generation of an OCSP Response of SigG-conforming client	☐	☒	
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	☐	☒	
	PKCS#11			
37	PKCS#11 general functions	☐	☒	
38	PKCS#11 functions for slot- and token management	☐	☒	
39	PKCS#11 functions for session management	☐	☒	
40	PKCS#11 functions for session management – optional	☐	☒	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: MICROSOFT WINDOWS SERVER 2003 CERTIFICATE SERVICE 2.0, MICROSOFT CORPORATION				
REFERENCE NUMBER: SECORVO-00003				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
	functions			
41	PKCS#11 functions for object management	☐	☒	
42	PKCS#11 functions for encryption	☐	☒	
43	PKCS#11 functions for decryption	☐	☒	
44	PKCS#11 functions for message digesting	☐	☒	
45	PKCS#11 functions for signing	☐	☒	
46	PKCS#11 functions for signing – optional functions	☐	☒	
47	PKCS#11 functions for verification	☐	☒	
48	PKCS#11 functions for verification – optional functions	☐	☒	
49	PKCS#11 functions for combined cryptographic operations	☐	☒	
50	PKCS#11 functions for combined cryptographic operations – optional functions	☐	☒	
51	PKCS#11 functions for key management	☐	☒	
52	PKCS#11 functions for generation of random numbers	☐	☒	
53	PKCS#11 functions for parallel functions management	☐	☒	
54	PKCS#11 functions for stubs	☐	☒	

Remark: It shall be noted that all functional classes without claimed support (i.e., all classes in which NO is marked in the lines 1 to 54) were not considered during this assessment. It does **NOT** necessarily mean that the functional classes are not supported by the Certificate Service.

6 Annex I: Test Log

6.1 Issuer Certificate

Starting Test Session for: Holger Mack

Date: Tue Mar 9 12:39:46 CET 2004

Component Under Test
Manufacturer: Microsoft Corporation
Product Name: Certificate Service, Enterprise CA
Version: Windows Server 2003
Remarks:
Enterprise Root CA Certificate

Starting test case TCGPKC-1
Date: Tue Mar 9 12:41:40 CET 2004
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1
Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed
Remarks: signature algorithm "sha1withRSAEncryption"
Test step 3 (signature) -- passed
Test step 4 (version) -- passed
Remarks: Version: v3
Test step 5 (serialNumber) -- passed
Test step 6 (issuer) --

Starting test case TCGDNAMES-1
Date: Tue Mar 9 12:41:42 CET 2004
Test step 1 (all attributes) -- passed
Remarks: Types and formats okay
Test step 2 (DirectoryString) -- failed
Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.
Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 12:41:42 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 12:41:42 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 12:41:42 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 9 (subjectPublicKeyInfo) -- passed

Remarks: Public key algorithm "rsaEncryption"

Test step 10 (issuerUniqueID) -- passed

Test step 11 (subjectUniqueID) -- passed

Test step 12 (extensions) --

Starting test case TCGEXTENSIONS-1

Date: Tue Mar 9 12:41:42 CET 2004

Test step 1 (all extensions) -- passed with warning

Remarks: Extension(s) "cAKeyCertIndexPair" present

Test step 2 (AuthorityKeyIdentifier) -- passed

Remarks: AuthorityKeyIdentifier not present

Test step 3 (SubjectKeyIdentifier) -- passed

Remarks: SubjectKeyIdentifier present

Test step 4 (KeyUsage) -- passed

Remarks: KeyUsage present

Test step 5 (PrivateKeyUsagePeriod) -- passed

Remarks: PrivateKeyUsagePeriod not present

Test step 6 (CertificatePolicies) -- passed

Remarks: CertificatePolicies not present

Test step 7 (SubjectAltNames) -- passed

Remarks: SubjectAltNames not present

Test step 8 (IssuerAltNames) -- passed

Remarks: IssuerAltNames not present

Test step 9 (SubjectDirectoryAttributes) -- passed

Remarks: SubjectDirectoryAttributes not present

Test step 10 (BasicConstraints) -- passed

Remarks: BasicConstraints present

Test step 11 (NameConstraints) -- passed

Remarks: NameConstraints not present

Test step 12 (PolicyConstraints) -- passed

Remarks: PolicyConstraints not present

Test step 13 (ExtendedKeyUsage) -- passed

Remarks: ExtendedKeyUsage not present

Test step 14 (CRLDistributionPoints) -- passed

Remarks: CRLDistributionPoints present

Test step 15 (AuthorityInfoAccess) -- passed

Remarks: AuthorityInfoAccess not present

Test step 16 (BiometricData) -- passed

Remarks: BiometricData not present

Test step 17 (QCStatements) -- passed

Remarks: QCStatements not present

Test step 18 (OCSPNocheck) -- passed

Remarks: OCSPNocheck not present

End of test case TCGEXTENSIONS-1
Test case passed with warning
Date: Tue Mar 9 12:41:42 CET 2004

passed with warning
End of test case TCGPKC-1
Test case failed
Date: Tue Mar 9 12:41:42 CET 2004

6.2 Sub CA Certificate

Starting Test Session for: Holger Mack

Date: Tue Mar 9 15:38:52 CET 2004

Component Under Test
Manufacturer: Microsoft Corporation
Product Name: Certificate Service
Version: Windows Server 2003
Remarks:
Sub CA (Template ISIS-MTT Assessment Sub CA)

Starting test case TCGPKC-1
Date: Tue Mar 9 15:39:11 CET 2004
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1
Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed
Remarks: signature algorithm "sha1withRSAEncryption"
Test step 3 (signature) -- passed
Test step 4 (version) -- passed
Remarks: Version: v3
Test step 5 (serialNumber) -- passed
Test step 6 (issuer) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 15:39:12 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 15:39:12 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 15:39:12 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 15:39:12 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 9 (subjectPublicKeyInfo) -- passed

Remarks: Public key algorithm "rsaEncryption"
Test step 10 (issuerUniqueID) -- passed
Test step 11 (subjectUniqueID) -- passed
Test step 12 (extensions) --

Starting test case TCGEXTENSIONS-1
Date: Tue Mar 9 15:39:12 CET 2004
Test step 1 (all extensions) -- passed with warning
Remarks: Extension(s) "unknown" present
Test step 2 (AuthorityKeyIdentifier) -- passed
Remarks: AuthorityKeyIdentifier present
Test step 2/a (keyIdentifier) -- passed
Remarks: keyIdentifier present
Test step 2/b (AuthorityCertIssuer) -- passed
Remarks: AuthorityCertIssuer not present
Test step 2/c (AuthorityCertSerialNumber) -- passed
Remarks: AuthorityCertSerialNumber not present
Test step 3 (SubjectKeyIdentifier) -- passed
Remarks: SubjectKeyIdentifier present
Test step 4 (KeyUsage) -- passed
Remarks: KeyUsage present
Test step 5 (PrivateKeyUsagePeriod) -- passed
Remarks: PrivateKeyUsagePeriod not present
Test step 6 (CertificatePolicies) -- passed
Remarks: CertificatePolicies not present
Test step 7 (SubjectAltNames) -- passed
Remarks: SubjectAltNames not present
Test step 8 (IssuerAltNames) -- passed
Remarks: IssuerAltNames not present
Test step 9 (SubjectDirectoryAttributes) -- passed
Remarks: SubjectDirectoryAttributes not present
Test step 10 (BasicConstraints) -- passed
Remarks: BasicConstraints present
Test step 11 (NameConstraints) -- passed
Remarks: NameConstraints not present

Test step 12 (PolicyConstraints) -- passed
Remarks: PolicyConstraints not present
Test step 13 (ExtendedKeyUsage) -- passed
Remarks: ExtendedKeyUsage not present
Test step 14 (CRLDistributionPoints) -- passed
Remarks: CRLDistributionPoints present
Test step 15 (AuthorityInfoAccess) -- failed
Remarks: Illegal AccessMethod "caIssuers"
Test step 16 (BiometricData) -- passed
Remarks: BiometricData not present
Test step 17 (QCStatements) -- passed
Remarks: QCStatements not present
Test step 18 (OCSPNocheck) -- passed
Remarks: OCSPNocheck not present
End of test case TCGEXTENSIONS-1
Test case failed
Date: Tue Mar 9 15:39:12 CET 2004

failed
End of test case TCGPKC-1
Test case failed
Date: Tue Mar 9 15:39:12 CET 2004

6.3 End Entity Certificate

Starting Test Session for: Holger Mack

Date: Tue Mar 9 13:37:47 CET 2004

Component Under Test
Manufacturer: Microsoft Corporation
Product Name: Windows Server 2003 Certificate Service
Version: Windows Server 2003
Remarks:

User Certificate (Template ISIS-MTT Assessment User)

Starting test case TCGPKC-1

Date: Tue Mar 9 13:38:07 CET 2004

Test step 1.1 (parse ASN.1) -- passed

Test step 1.2 (parse ASN.1
Issuer Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (version) -- passed

Remarks: Version: v3

Test step 5 (serialNumber) -- passed

Test step 6 (issuer) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 13:38:07 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 13:38:07 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 13:38:07 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) commonName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 13:38:07 CET 2004

failed

Remarks: CountryName is missing

Test step 9 (subjectPublicKeyInfo) -- passed

Remarks: Public key algorithm "rsaEncryption"

Test step 10 (issuerUniqueID) -- passed

Test step 11 (subjectUniqueID) -- passed

Test step 12 (extensions) --

Starting test case TCGEXTENSIONS-1

Date: Tue Mar 9 13:38:07 CET 2004

Test step 1 (all extensions) -- passed with warning

Remarks: Extension(s) "unknown", "unknown" present

Test step 2 (AuthorityKeyIdentifier) -- passed

Remarks: AuthorityKeyIdentifier present

Test step 2/a (keyIdentifier) -- passed

Remarks: keyIdentifier present

Test step 2/b (AuthorityCertIssuer) -- passed

Remarks: AuthorityCertIssuer not present

Test step 2/c (AuthorityCertSerialNumber) -- passed

Remarks: AuthorityCertSerialNumber not present

Test step 3 (SubjectKeyIdentifier) -- passed

Remarks: SubjectKeyIdentifier present

Test step 4 (KeyUsage) -- passed

Remarks: KeyUsage present

Test step 5 (PrivateKeyUsagePeriod) -- passed
Remarks: PrivateKeyUsagePeriod not present
Test step 6 (CertificatePolicies) -- passed
Remarks: CertificatePolicies not present
Test step 7 (SubjectAltNames) --

Starting test case TCGGENNAMES-1
Date: Tue Mar 9 13:38:07 CET 2004
Test step 1 (otherName) -- passed
Remarks: otherName not present
Test step 2 (rfc822Name) -- passed
Remarks: rfc822Name present
Test step 3 (dNSName) -- passed
Remarks: dNSName not present
Test step 4 (x400Name) -- passed
Remarks: x400Name not present
Test step 5 (directoryName) -- passed
Remarks: directoryName not present
Test step 6 (ediPartyName) -- passed
Remarks: ediPartyName not present
Test step 7 (uniformResourceIdentifier) -- passed
Remarks: ipAddress not present
Test step 8 (iPAddress) -- passed
Remarks: ipAddress not present
Test step 9 (registeredID) -- passed
Remarks: registeredID not present
End of test case TCGGENNAMES-1
Test case passed
Date: Tue Mar 9 13:38:07 CET 2004

passed
Remarks: SubjectAltNames present
Test step 8 (IssuerAltNames) -- passed
Remarks: IssuerAltNames not present
Test step 9 (SubjectDirectoryAttributes) -- passed

Remarks: SubjectDirectoryAttributes not present
Test step 10 (BasicConstraints) -- passed
Remarks: BasicConstraints not present
Test step 11 (NameConstraints) -- passed
Remarks: NameConstraints not present
Test step 12 (PolicyConstraints) -- passed
Remarks: PolicyConstraints not present
Test step 13 (ExtendedKeyUsage) -- passed with warning
Remarks: KeyPurposeId(s) "encryptedFileSystem" present
Test step 14 (CRLDistributionPoints) -- passed
Remarks: CRLDistributionPoints present
Test step 15 (AuthorityInfoAccess) -- failed
Remarks: Illegal AccessMethod "caIssuers"
Test step 16 (BiometricData) -- passed
Remarks: BiometricData not present
Test step 17 (QCStatements) -- passed
Remarks: QCStatements not present
Test step 18 (OCSPNocheck) -- passed
Remarks: OCSPNocheck not present
End of test case TCGEXTENSIONS-1
Test case failed
Date: Tue Mar 9 13:38:07 CET 2004

failed
End of test case TCGPKC-1
Test case failed
Date: Tue Mar 9 13:38:07 CET 2004

6.4 CRL

Starting Test Session for: Holger Mack

Date: Tue Mar 9 13:49:12 CET 2004

Component Under Test

Manufacturer: Microsoft Corporation

Product Name: Certificate Service

Version: Windows Server 2003

Remarks:

Full CRL

Starting test case TCGCRL-1

Date: Tue Mar 9 13:49:44 CET 2004

Test step 1.1 (parse ASN.1
CertificateList) -- passed

Test step 1.2 (parse ASN.1
Issuer Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (issuer) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 13:49:45 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 13:49:45 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 5 (thisUpdate) -- passed

Test step 6 (nextUpdate) -- passed

Test step 7 (revokedCertificates) -- passed

Remarks: revokedCertificates present
Test step 7/a (userCertificate) -- passed
Test step 7/b (revocationDate) -- passed
Test step 7/c (crlEntryExtensions) --

Starting test case TCGEXTENSIONS-1
Date: Tue Mar 9 13:49:45 CET 2004
Test step 1 (all extensions) -- passed
Test step 22 (ReasonCode) -- passed
Test step 23 (HoldInstructionCode) -- passed
Test step 24 (InvalidityDate) -- passed
Test step 25 (CertificateIssuer) -- passed
End of test case TCGEXTENSIONS-1
Test case passed
Date: Tue Mar 9 13:49:45 CET 2004

passed
Test step 8 (crlExtensions) --

Starting test case TCGEXTENSIONS-1
Date: Tue Mar 9 13:49:45 CET 2004
Test step 1 (all extensions) -- passed with warning
Remarks: Extension(s) "cAKeyCertIndexPair", "unknown", "unknown", "unknown" present
Test step 2 (AuthorityKeyIdentifier) -- passed with warning
Remarks: AuthorityKeyIdentifier present in direct CRL
Test step 2/a (keyIdentifier) -- passed
Remarks: keyIdentifier present
Test step 2/b (AuthorityCertIssuer) -- passed
Remarks: AuthorityCertIssuer not present
Test step 2/c (AuthorityCertSerialNumber) -- passed
Remarks: AuthorityCertSerialNumber not present
Test step 8 (IssuerAltNames) -- passed
Remarks: IssuerAltNames not present
Test step 19 (CRLNumber) -- passed
Remarks: CRLNumber present

Test step 20 (DeltaCRLIndicator) -- passed
Remarks: DeltaCRLIndicator not present
Test step 21 (IssuingDistributionPoint) -- passed
Remarks: IssuingDistributionPoint not present
End of test case TCGEXTENSIONS-1
Test case passed with warning
Date: Tue Mar 9 13:49:45 CET 2004

passed with warning
End of test case TCGCRL-1
Test case failed
Date: Tue Mar 9 13:49:45 CET 2004

6.5 Delta-CRL

Starting Test Session for: Holger Mack

Date: Tue Mar 9 17:48:48 CET 2004

Component Under Test
Manufacturer: Microsoft Corporation
Product Name: Certificate Service
Version: Windows Server 2003
Remarks:
Delta CRL

Starting test case TCGCRL-1
Date: Tue Mar 9 17:49:30 CET 2004
Test step 1.1 (parse ASN.1
CertificateList) -- passed
Test step 1.2 (parse ASN.1
Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (issuer) --

Starting test case TCGDNAMES-1

Date: Tue Mar 9 17:49:31 CET 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- failed

Remarks: Encoding of attribute(s) organizationName, organizationalUnitName, commonName must be UTF8String from year 2004 on.

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case failed

Date: Tue Mar 9 17:49:31 CET 2004

failed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 5 (thisUpdate) -- passed

Test step 6 (nextUpdate) -- passed

Test step 7 (revokedCertificates) -- passed

Remarks: revokedCertificates present

Test step 7/a (userCertificate) -- passed

Test step 7/b (revocationDate) -- passed

Test step 7/c (crlEntryExtensions) --

Starting test case TCGEXTENSIONS-1

Date: Tue Mar 9 17:49:31 CET 2004

Test step 1 (all extensions) -- passed

Test step 22 (ReasonCode) -- passed

Test step 23 (HoldInstructionCode) -- passed

Test step 24 (InvalidityDate) -- passed

Test step 25 (CertificateIssuer) -- passed

End of test case TCGEXTENSIONS-1
Test case passed
Date: Tue Mar 9 17:49:31 CET 2004

passed
Test step 8 (crlExtensions) --

Starting test case TCGEXTENSIONS-1
Date: Tue Mar 9 17:49:31 CET 2004
Test step 1 (all extensions) -- passed with warning
Remarks: Extension(s) "cAKeyCertIndexPair", "unknown", "unknown" present
Test step 2 (AuthorityKeyIdentifier) -- passed with warning
Remarks: AuthorityKeyIdentifier present in direct CRL
Test step 2/a (keyIdentifier) -- passed
Remarks: keyIdentifier present
Test step 2/b (AuthorityCertIssuer) -- passed
Remarks: AuthorityCertIssuer not present
Test step 2/c (AuthorityCertSerialNumber) -- passed
Remarks: AuthorityCertSerialNumber not present
Test step 8 (IssuerAltNames) -- passed
Remarks: IssuerAltNames not present
Test step 19 (CRLNumber) -- passed
Remarks: CRLNumber present
Test step 20 (DeltaCRLIndicator) -- passed
Remarks: DeltaCRLIndicator present
Test step 21 (IssuingDistributionPoint) -- passed
Remarks: IssuingDistributionPoint not present
End of test case TCGEXTENSIONS-1
Test case passed with warning
Date: Tue Mar 9 17:49:31 CET 2004

passed with warning
End of test case TCGCRL-1
Test case failed
Date: Tue Mar 9 17:49:31 CET 2004